IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA

v.

STEPHEN GORDON GRIMES, JR.

CRIMINAL CASE

No. 1:20-CR-00427-SCJ

ORDER

This matter appears before the Court on Defendant's Objections to the Magistrate Court's Report and Recommendation to deny the suppression of evidence obtained in, and from, a search of his electronic devices.[1] Doc. No. [73]. The Court hereby **OVERRULES** Defendant's objections and **ADOPTS** The Magistrate's recommendation (Doc. No. [45]). The Court thus **DENIES** Defendant's motion to suppress. Doc. No. [26].

---

[1] All citations are to the electronic docket unless otherwise noted, and all page numbers are those imprinted by the Court's docketing software.

I. BACKGROUND

On September 29, 2020, Defendant flew into the Atlanta airport from South Korea. Doc. No. [32] (Suppression Hearing Tr.) Tr. 9:14–22. During his preliminary processing to enter the United States, Defendant presented his U.S. passport and did not show any signs of suspicious activity. Id. at 10:8–13, 18:6–7. Part of the airport's preliminary processing involves the use of a facial recognition technology to identify entrants who might be associated with criminal activity, such as possession of child exploitation materials. Id. at 8:11–24, 11:1–3. An entrant identified by this facial recognition technology is called a "lookout." Id. at 11:4–13.

Agents used this facial recognition technology as Defendant was being processed and he returned as a lookout linked to child sexual exploitation material. Id. at 10:24–11:17. Based on this information, the agents took Defendant to secondary processing where they searched his baggage and examined his numerous electronic devices. Id. at 13:2–10, 27:19–21, 37:14–17. The lookout identification prompted the officers specifically to search Defendant's electronic devices. Id. at 55:1–3. During the 15- or 20-minute search of Defendant's electronic devices, the officers discovered recently deleted photos of young child

erotica. Id. at 31:14–25. At this point, the customs officers called Homeland Security, who then took over the investigation. Id. at 32:12–24.

Based on evidence obtained in, and from, this airport search, the Government indicted Defendant for using a minor to engage in sexually explicit conduct to produce a visual depiction of such conduct (18 U.S.C. § 2251(c)(2)(B)), attempting to transport a visual depiction of minors engaged in sexually explicit conduct (id. § 2252(a)(1)) and possessing a visual depiction of minors engaged in sexually explicit conduct (id. § 2252(a)(4)(B)). Doc. No. [20]. Trial has been scheduled to begin April 3, 2023. Doc. No. [70].

On May 7, 2021, Defendant moved to suppress the evidence obtained from the cell phone search. Doc. No. [26]. The Magistrate Court held a hearing on this motion on June 2, 2021. Doc. Nos. [30]; [32]. The Magistrate then recommended the Court deny Defendant's motion to suppress, reasoning that binding Eleventh Circuit precedent foreclosed Defendant's argument for suppression. Doc. No. [45], 6–7. The time for objections to the report and recommendation expired, the Court entered an order adopting the Magistrate's recommendation. Doc. No. [52]. Over a year passed before Defendant filed a consent motion to reopen the period for objections. Doc. No. [69]. Despite having reservations about

a lack of good cause, the Court granted Defendant's motion because the Government had consented to it. Doc. No. [72], 1 n.2. Defendant thereafter filed his objections to the Magistrate's recommendation, and the Government responded in opposition. Doc. Nos. [73]; [74]. The Court now turns to Defendant's objections to the Magistrate's recommendation.

II. LEGAL STANDARD

"When a party files proper objections [to a Magistrate's Report and Recommendation], the Court must "make a *de novo* determination of those portions of the report or specified proposed findings or recommendations to which objection is made." 28 U.S.C. § 636(b)(1). Parties filing objections must specifically identify the findings in which they object. Marsden v. Moore, 847 F.2d 1536, 1548 (11th Cir. 1988). After conducting its *de novo* review, the Court "may accept, reject, or modify in whole or in part, the findings or recommendations made by the magistrate judge." Id. The Court reviews the uncontested portions of the Recommendation for clear error. 28 U.S.C. § 636(b)(1); see also Fed. R. Civ. P. 72(b); Middleburg Mgmt., LLC v. Wright, No. 1:19-CV-03518-SDG, 2020 WL 7405668, at *1 (N.D. Ga. Mar. 27, 2020).

III. ANALYSIS

Defendant raises two objections to the Magistrate's recommendation: (1) that officers should be legally required to have reasonable suspicion to conduct a border search of an electronic device, and (2) that there was no reasonable suspicion to conduct the searches of Defendant's devices in this case. Doc. No. [73], 4–8. The Government, for its part, relies on binding Eleventh Circuit precedent, which does not require reasonable suspicion for border searches of cell phones. Doc. No. [74], 2. The Government alternatively argues that even if reasonable suspicion is required, the officers here had reasonable suspicion for this search based on the lookout identification linking Defendant to child exploitation materials. Id. at 4–5.

The Magistrate denied Defendant's motion to suppress based on the Eleventh Circuit precedent and reserved any ruling on the reasonable suspicion issue. Doc. No. [45], 6–7. The Court here, however, chooses to address both issues. The Court ultimately determines that both of Defendant's objections must be overruled and the motion to suppress denied.

A. Reasonable Suspicion Is Not Required for Border Searches of Electronic Devices

Defendant objects to the lack of reasonable suspicion supporting the border search of his electronic devices for purposes of preserving the issue for appeal. Both Parties and the Court agree that the Eleventh Circuit does not require reasonable suspicion for border searches of electronic devices. See United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property."); cf. also United States v. Vergara, 884 F.3d 1309, 1312–13 (11th Cir. 2018) (rejecting the contention that a warrant or probable cause is required for forensic or manual searches of phones in the light of Riley v. California, 134 S. Ct. 2473 (2014));.

Given these binding precedents, which Defendant acknowledges precludes suppression of the cell phone evidence in this case, the Court overrules Defendant's objection and adopts the Magistrate's recommendation to deny Defendant's suppression motion.

B. Reasonable Suspicion Existed to Search Defendant's Phones

The Court will also address the Government's alternative argument that even if reasonable suspicion was required for this search, the officers here had such suspicion to search Defendant's phones given the lookout linking Defendant to child exploitation materials.[2] Doc. No. [74], 4–5. Defendant contends that there was no reasonable suspicion because the Government has offered no evidence that the facial recognition program the officers relied on to begin the search of Defendant's devices was reliable. Doc. No. [73], 6–7. Defendant analogizes the lack of reliability of a database to an unverified anonymous tip. Id. at 7–8.

Defendant's arguments do not persuade the Court in the light of the evidence presented at the suppression hearing in this case. It is true that the

---

[2] Defendant also challenges reasonable suspicion based on the four images of child erotica found on his cell phone. Doc. No. [73], 9–11. While there is a critical difference in the possession of child erotica and the possession of child pornography, Defendant's argument misses the mark in terms of suppressing of the contents from the cell phone search. Assuming reasonable suspicion is required, the question is whether the officers had such suspicion *prior* to the cell phone searches. The child erotica was found *during* the search. This issue may be relevant for determining if the officers' exceeded their reasonable suspicion by conducting a prolonged search, but Defendant has made no such contention. Accordingly, any argument that the photographs are child erotica (not child pornography) does not support Defendant's argument that there was a lack of reasonable suspicion for initiating the search of his devices.

officers who engaged with Defendant during the search did not perceive anything suspicious about his behavior prior to the lookout. Doc. No. [32] (Suppression Hearing Tr.) Tr. 18:6–7. Reasonable suspicion, however is a "less demanding" standard that "depends on the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Kansas v. Glover, 140 S. Ct. 1183, 1188 (2020) (quoting Alabama v. White, 496 U.S. 325, 330 (1990) and Navarette v. California, 572 U.S. 393, 402 (2014)).

The Eleventh Circuit has allowed officers to rely on information from database searches as a basis for reasonable suspicion. Cf., e.g., United States v. Gardner, 444 F. App'x 361, 362 (11th Cir. 2011) (affirming reasonable suspicion existed even when an officer relied on information from a database search that occurred 2-weeks prior); Brims v. Barlow, 441 F. App'x 674, 677–78 (11th Cir. 2011) (affirming reasonable suspicion when a defendant "did not dispute that his registration was listed as being suspended in the police database . . . ."); United States v. Ochoa, 402 F. App'x 478, 483 (11th Cir. 2010) (relying on "multiple criminal, immigration, credit-check, and identity databases" in finding reasonable suspicion)

Indeed, in most of these cases affirming reasonable suspicion based on a database search the officers had other verifications of the database evidence. But such verification is not completely lacking in this case. The officer who conducted the secondary search of Defendant's electronic devices indicated that, while nothing in the communications with Defendant was suspicious, "the excessive amount of electronic media that he had was a little off." Doc. No. [32] (Suppression Hearing Tr.) Tr. 36:1–2. This "excessive" number of devices, in addition to the lookout linking Defendant to child exploitation materials is sufficient for the Court to find that there was a "minimal level of objective justification" for the search initiated. United States v. Bruce, 977 F.3d 1112, 1116–17 (11th Cir. 2020) (quoting Illinois v. Wardlow, 528 U.S. 119, 123 (2000)). This conclusion is reinforced by the fact that the record is devoid of any evidence that the facial recognition database in this case was unreliable[3]—a critical

[3] "[T]he Government bears the burden of establishing reasonable suspicion or probable cause for the seizure at a suppression hearing." United States v. Longoria, 183 F. Supp. 3d 1164, 1170 (N.D. Fla. 2016) (citing United States v. de la Fuente, 548 F.2d 528, 533 (5th Cir. 1977)). The Court here finds that the officers' testimony about the "national targeting center" and "headquarters" entering the information, which the officers relied on without any indication that the information was error-prone, as sufficient to satisfy the "less demanding" burden of proof for reasonable suspicion in this case. Doc. No. [32] (Suppression Hearing Tr.) Tr. 37:18–21, 38:20–21.

distinction made in the Tenth Circuit case Defendant relies on in his argument (Doc. No. [73], 6–7). See United States v. Esquivel-Rios, 725 F.3d 1231, 1237–38 (10th Cir. 2013) (finding that given an officer's comment that the type of vehicle tag at issue "usually [didn't] return" in the database searched, the district court committed error in "treat[ing] this case as just another one where the database wasn't challenged."). Here, conversely, there is no suggestion from the officers that the lookout obtained from the facial recognition technology was inaccurate or prone to error.

Thus, the Court alternatively determines that the officers had a reasonable suspicion to search Defendant's electronic devices, based (primarily) on the facial recognition's lookout identification, the number of devices in Defendant's possession, and the lack of any suggestion by the officers that they had reason to suspect the data returned on Defendant or that the database was erroneous.

IV. CONCLUSION

For the foregoing reasons, the Court **OVERRULES** Defendant's objections to the Magistrate Court's report and recommendation. Doc. No. [73]. The Court **ADOPTS** the Magistrate's recommendation (Doc. No. [45]), subject to the additional conclusions contained in this Order. Accordingly, Defendant's motion

to suppress the evidence from the search of his cell phone is **DENIED**. Doc. No. [32].

IT IS SO ORDERED this 10th day of March, 2023.

Steve C. Jones

HONORABLE STEVE C. JONES
UNITED STATES DISTRICT JUDGE